U.S. Application No. 09/457,732   2
Docket No. YOR919990137US1
(YOR.080)

AMENDMENTS TO THE CLAIMS:

1.   (Currently amended) A method of processing semiotic data, comprising:

receiving semiotic data including a data set P;

selecting a function h, and for at least one of each said data set P to be collected,

computing h(P);

destroying said data set P;

storing h(P) in a database, and

to determine whether P' is <u>close to</u> a predetermined subject, comparing h(P') to available

h(P)s to determine whether <u>P' is close to some P</u> ~~there is a match~~,

wherein said data set P cannot be extracted from h(P).

2.   (Original) The method according to claim 1, wherein said semiotic data comprises

biometric data.

3.   (Original) The method according to claim 1, wherein said function h comprises a secure

hash function.

4.   (Canceled).

5.   (Previously presented) A method of processing semiotic data, comprising:

receiving semiotic data including a data set P;

selecting a function h, and for at least one of each said data set P to be collected,

computing h(P);

destroying said data set P; and

storing h(P) in a database,

wherein said data set P cannot be extracted from h(P),

the method further comprising:

selecting a private key/public key (K, k) once for all cases; and

one of destroying said private key K and sending said private key K to a trusted party;

and

choosing said function h as the public encryption function corresponding to k.

6.   (Original) The method according to claim 5, wherein said data set P cannot be extracted

from h(P), except by the trusted party.

7.   (Previously presented) The method according to claim 5, further comprising:

to determine whether some P' is a predetermined subject, comparing said h(P') to

available h(P)s; and

determining whether there is a match.

8.   (Original) The method according to claim 5, wherein the trusted party comprises a panel

of members, and

wherein a secret is shared among the members so that only at least a predetermined

number of panel members can reconstitute the secret in its entirety by putting together their share

of the secret.

9.   (Previously presented) A method of processing semiotic data, comprising:

receiving semiotic data including a data set P;

selecting a function h, and for at least one of each said data set P to be collected,

computing h(P);

destroying said data set P; and

storing h(P) in a database,

wherein said data set P cannot be extracted from h(P),

wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number P_i, wherein i is no less than 0, wherein $P0$ is for an

initial reading, and a secret version of said initial reading is stored after further processing

thereof,

wherein reading $P0$ is different from P_i for i > 0, and the secret version of $P0$ is different

from the secret version of P_i, such that no identification is possible by a direct comparison of the

encrypted data.

10.   (Original) The method according to claim 9, further comprising:

extracting sub-collections S_j from the collection of data in data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the

sub-collections is reproduced exactly with a predetermined probability.

11.   (Original) The method according to claim 10, further comprising:

comparing encrypted versions of the sub-collections S_j with those data stored in said

database,

wherein if one or more of the sub-collection Sj matches with said data, then verification

is deemed to have occurred.

12.   (Original) The method according to claim 11, further comprising:

each time a Pi, with i > 0, is read, computing all possible predetermined size variations of

Pi which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data

stored in said database.

13.   (Original) The method according to claim 12, wherein for a plurality of users of the same

biometric information, said biometric information is encrypted differently for each user.

14.   (Previously presented) The method according to claim 1, wherein at least one of said data

set P and P' comprises a personal data set.

15.   (Previously presented) A method of processing biometric data, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting, with one of a secure hash function and an identity function, each said at least

one data set acquired;

destroying the unencrypted data set P;

storing each of the at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored

in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted

data set of P' to the at least one encrypted data set stored in the database to determine whether

there is a match.

16.   (Previously presented) The method according to claim 15, wherein at least one of said

data set P and P' comprises a personal data set.

17.   (Previously presented) A method of extracting components of biometric data which are

stable under measurement errors, comprising:

     acquiring unencrypted biometric data including at least one data set P;

     encrypting each said at least one data set acquired to form at least one encrypted data set;

     destroying the unencrypted data set P;

     storing each said at least one encrypted data set in a database,

     wherein unencrypted biometric data is not available nor retrievable from said data stored

in said database, and

     to determine whether a data set P' is a predetermined subject, comparing an encrypted

data set of P' to the at least one encrypted data set stored in the database to determine whether

there is a match.

18.   (Previously presented) The method according to claim 17, wherein at least one of said

data set P and P' comprises a personal data set.

19.   (Original) A method of extracting components of biometric data which are stable under

measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored

in said database,

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the

sub-collections is reproduced exactly with a predetermined probability.

20.   (Original) The method according to claim 19, wherein said data set comprises a personal

data set.

21.   (Original) The method according to claim 19, further comprising:

comparing encrypted versions of the sub-collections Sj with those data stored in said

database,

wherein if one or more of the sub-collection Sj matches with said data, then verification

is deemed to have occurred.

22.   (Original) The method according to claim 21, wherein a data set P is not determined

perfectly by its reading, such that each reading gives a number Pi,

wherein i is no less than 0,

wherein P0 is for an initial reading, and a secret version of said initial reading is stored

after further processing thereof,

wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different

from the secret version of Pi, such that no identification is possible by a direct comparison of the

encrypted data.

23.   (Original) The method according to claim 21, further comprising:

each time a data set is read Pi, with i > 0, is read, computing all possible predetermined

size variations of Pi which correspond to an acceptable predetermined imprecision of the

reading; and

encrypting all such modified data, and comparing said encrypted modified data to data

stored in said database.

24.   (Currently amended) A system for processing semiotic data, comprising:

means for receiving semiotic data including a data set P;

means for selecting a function h, and for each said data set P to be collected, computing

h(P);

means for destroying said data set P;

means for storing h(P) in a database, wherein said data set P cannot be extracted from

h(P), and

to determine whether a data set P' is <u>close to</u> a predetermined subject, means for

comparing h(P') to available h(P)s to determine whether <u>data set P' is close to some P</u> ~~there is a~~

~~match.~~

25.   (Previously presented) A system of processing semiotic data as in claim 24, wherein said

semiotic data comprises biometric data.

26.   (Previously presented) The method according to claim 24, wherein at least one of said

data set P and P' comprises a personal data set.

27.   (Previously presented) A system for verifying biometric data without storing unencrypted

biometric data, comprising:

    means for acquiring unencrypted biometric data including at least one data set P;

    means for encrypting each said at least one data set acquired to form at least one

encrypted data set; means for destroying the unencrypted data set P;

    means for storing each said at least one encrypted data set in a database, wherein

unencrypted biometric data is not available nor retrievable from said data stored in said database,

and

    means for comparing an encrypted data set of a data set P' to said at least one encrypted

data set of data set P to determine whether there is a match and to determine whether the data set

P' is a predetermined subject.

U.S. Application No. 09/457,732   10
Docket No. YOR919990137US1
(YOR.080)

28.   (Previously presented) The method according to claim 27, wherein at least one of said

data set P and P' comprises a personal data set.

29.   (Original) A system for extracting components of biometric data which are stable under

measurement errors, comprising:

   acquiring unencrypted biometric data including at least one data set P; encrypting each

said at least one data set acquired to form at least one encrypted data set;

   destroying the unencrypted data set P; and

   storing each said at least one encrypted data set in a database,

   wherein unencrypted biometric data is not available nor retrievable from said data stored

in said database,

   extracting sub-collections Sj from the collection of data in said data set P; and

   encrypting a predetermined number of such sub-collections such that at least one of the

sub-collections is reproduced exactly with a predetermined probability.

30.   (Original) The method according to claim 29, wherein said data set comprises a personal

data set.

31.   (Currently amended) A signal-bearing medium tangibly embodying a program of

machine-readable instructions executable by a digital processing apparatus to perform a method

for computer-implemented processing biometric data, said method comprising:

   receiving biometric data including a data set P;

selecting a secure hash function h, and for each data set P to be collected, computing

h(P);

destroying said data set P;

storing h(P) in a database, wherein said data set P cannot be extracted from h(P), and

to determine whether a data set P' is <u>close to</u> a predetermined subject, comparing h(P') to

available h(P)s to determine whether <u>data set P' is close to some data set P</u> ~~there is a match~~.

32.   (Previously presented) The method according to claim 31, wherein at least one of said

data set P and P' comprises a personal data set.

33.   (Currently amended) A signal-bearing medium tangibly embodying a program of

machine-readable instructions executable by a digital processing apparatus to perform a method

for computer-implemented verifying of biometric data without storing unencrypted biometric

data, said method comprising:

acquiring unencrypted biometric data including at least one data set P;

encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted

biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is <u>close to</u> a predetermined subject, comparing an

encrypted data set of P' to said at least one encrypted data set to determine whether <u>data set P' is</u>

<u>close to some data set P</u> ~~there is a match~~.

U.S. Application No. 09/457,732   12
Docket No. YOR919990137US1
(YOR.080)

34.   (Previously presented) The method according to claim 33, wherein at least one of said

data set P and P' comprises a personal data set.

35.   (Original) A signal-bearing medium tangibly embodying a program of machine-readable

instructions executable by a digital processing apparatus to perform a method for computer-

implemented extracting components of biometric data which are stable under measurement

errors, said method comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each

said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted

biometric data is not available nor retrievable from said data stored in said database;

extracting sub-collections Sj from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the

sub-collections is reproduced exactly with a predetermined probability.

36.   (Original) The method according to claim 35, wherein said data set comprises a personal

data set.